Amendments to the Specification:

At page 2, at line 18, before the title **BRIEF DESCRIPTION OF THE DRAWINGS**, please include the following Summary paragraphs:

SUMMARY

In one aspect, the invention features a gaming network including a plurality of gaming machines and one or more information servers coupled to the plurality of gaming machines. The one or more information servers are structured to store data related to the plurality of gaming machines and related to players of the gaming machines, and to generate data for use on the gaming network. The gaming network further includes a secure wireless server coupled to the one or more information servers and a secure wireless receiver. The secure wireless receiver is structured to couple to the secure wireless server and to create a secure data channel between the wireless server and the wireless receiver.

In another aspect, the invention features a system for redeeming tickets. The system includes one or more information servers on a gaming network. The one or more information servers are configured to store data related to past play of gaming machines and related to players of the gaming machines, and to generate data for use on the gaming network. The data stored on the one or more information servers relates to transactions previously memoralized by a ticket. The system further includes a wireless server coupled to the one or more information servers and a secure wireless receiver. The secure wireless receiver is structured to couple to the secure wireless server and create a secure data channel between the wireless server and the wireless receiver over which data stored on the one or more information servers can be retrieved.

Please replace the paragraph at page 7, lines 9-21, with the following amended paragraph:

Also shown in FIGs. 1 and 2 are a number of wireless servers 130, also referred to as wireless access points (WAPs). The wireless servers 130 transmit and receive RF (Radio Frequency) signals over the gaming floor 118, thereby communicating with one or more wireless devices 140. Example wireless servers 130 are those that adhering to IEEE 802.11b, 802.11a, or 802.11g protocols, but any acceptable communication protocol could be used. The wireless servers 130 are connected to each other via wires or wireless links, as is know in the art. The wireless servers 130 and wireless devices 140 illustrated in FIG. [[1]] 2 may be implemented as a same set of wireless servers 130 and wireless devices 140, or may, in fact, be separate systems, where the wireless devices 140 only communicate with a particular, and not all, wireless servers 130 in the game network 5. The wireless devices 140 both receive and transmit information to the wireless servers 130, as is known in the art.

Please replace the paragraph at page 7, line 28 to page 8, line 8, with the following amended paragraph:

The wireless servers 130 may be separated from the gaming network 5 by a firewall 150. A firewall is hardware and software operating to protect resources of a network. Specifically, the firewall 150 can be a tunneling firewall that encapsulates and encrypts data packets traveling between the wireless servers 130 and the firewall 150. An application server 110 can be used in conjunction with the wireless servers 130 on the gamefloor 118. Additionally, a switch 160 could be used to partition particular IP (Internet Protocol) or other addresses so the partitioned addresses are only available by the wireless servers 130, or the wireless devices 140 that couple to the wireless servers 130. Although illustrated outside of the gaming floor 118, the firewall 150, server 110, and switch 160 could all also be within the gaming floor ~~115~~ 118. Their physical location is unimportant.

Please replace the paragraph at page 8, lines 8-15, with the following amended paragraph:

With reference back to ~~Figure 1~~ Figure 1B, the application server ~~115~~ 110 of FIG. 2 could be embodied by a Mobile Data Access (MDA) server 108. The firewall 150 of FIG. 2 is not present in ~~FIG. 1~~ FIG. 1B but could, of course, be added between the MDA server 108 and the rest of the gaming network 5. In ~~FIG. 1~~ FIG. 1B, the MDA server 108 connects to the gaming network 5 through a communication hub 102. The communication hub 102, in turn, is connected to the translator 50 and to an event monitor 104. The event monitor 104 is also coupled to the server cluster 56, which was described above.

Please replace the paragraph at page 8, lines 27-32, with the following amended paragraph:

Operation of the wireless servers 130 and wireless devices 140 is described with reference to FIGS. [[1]] 1B, 2, and 3. Illustrated in FIG. 3 are different example levels of providing secure communication between a wireless server 130 or application server 110 and a wireless device 140. Of course, as described above, a wireless server 130 can communicate with many wireless devices 140 at the same time, as can the application server 110.

Please replace the paragraph at page 10, line31 to page 11, line 6, with the following amended paragraph:

In operation, when a wireless device 140 communicates to one of the wireless servers 130, it must first have the proper frequency, channel settings, ESSID, WEP keys, and MAC address. If any of these settings are not correct, the wireless server prohibits access and, if possible, creates a log of the event. In some embodiments, the wireless device 140 can create an alert for casino personnel to investigate if someone is trying to hack into the secure network.

Such an alert can be sent to an operator terminal at one of the bank controllers (FIG. [[1]] 1A), for example.

Please replace the paragraph at page 11, lines 7-24, with the following amended paragraph:

If the wireless device 140 has the proper frequency, channel settings, WEP key and MAC address, the DHCP server determines if the particular device should be allowed onto the wireless portion of the gaming network 5. A particular wireless device may only be authorized to log onto the gaming network 5 during particular times. The DHCP server monitors these actions and only allows the wireless device 140 to log in when so authorized. For instance, a particular device can be checked out to a particular employee. The DHCP server can be set up to allow a log in for that device only when that employee is scheduled to work. Or, the DHCP server can be set up to only allow a log in during the first 15 minutes of that employees shift. If the employee did not log in during that time period, the DHCP server could block any log in of that wireless device 140 until the employee met with a manager, who could re-enable the DHCP server to allow login. ~~additionally~~ Additionally, the DHCP server can be set up to automatically log out a previously logged in user who does not use the wireless device 140 for a period of time, for instance, for over 20 minutes. That prevents an unauthorized person from finding a misplaced wireless device 140 and taking advantage of the gaming network 5. Other detailed examples of using a wireless device are given below.

Please replace the paragraph at page 12, line29 to page 13, line 7, with the following amended paragraph:

A standard procedure for providing employees with wireless devices 140 in a casino gaming network 5 could be as follows, as described with reference to FIGs. [[1]] 1A, 1B, 2, 5, and 6. In FIGs. [[1]] 1A, 1B and 5, an exemplary application server 115, termed a "redemption" server, is shown. The redemption server 115 could be an embodiment of the generic server 110 of FIG. 2. Although only a single server 110 is illustrated in FIG. 2, in practice any number of servers 110 could be implemented. The redemption server 115 can couple to the gaming network 5 (FIG [[1]] 1A, 1B) as shown in FIG. 2. Specifically, the redemption server 115 can couple to the server cluster 56, which provides access to the databases 100. In one embodiment, the redemption server 115 only couples to the slot accounting database 90 and the ticket wizard database 94.

Please replace the paragraph at page 13, lines 8-16, with the following amended paragraph:

The redemption server 115 primarily functions to redeem tickets or other redeemable rewards. Referring back to FIG. 5, included in the redemption server 115 are two NIC (Network Interface Cards) cards connected by a software bridge. One of the NIC cards, for example NIC 1, is coupled to and communicates with the gaming network 5, including being able to access the data stored on databases 100, for instance. The other NIC card, NIC 2, communicates with the wireless communication portion of the network. The NIC 2 is coupled to a wireless access point 130, which is also illustrated in FIGs [[1]] 1A, 1B and 2. A software bridge communicates requests and data from one network portion to the other.

Please replace the paragraph at page 16, lines 21-29, with the following amended paragraph:

One problem that could prevent the entered ticket number from being validated is if the bar code or other type of reader was not operating properly at the wireless device 140. Of course, there is also the possibility that the ticket was made fraudulently, and therefore the ticket number cannot be validated by a corresponding database entry. Also, a player may unscrupulously try to photocopy, or otherwise ~~made~~ make multiple copies of a ticket. Because, as described below, once a ticket has been redeemed it is marked as such in the gaming network 5, presenting a ticket that has already been redeemed is also another reason that a ticket number would not be validated.